Why does Cyber Crucible respond by suspending a process instead of shutting down the system?

Short answer: Suspending only the malicious process — sometimes called a Selective Freeze — neutralizes the attack while everything else keeps running. There's no full-system lockdown, no reboot, and no interruption to legitimate work.

The problem with lockdown-style responses

When many detection tools identify an anomaly, the containment options are blunt: isolate the machine or take it offline. In a hospital, a plant, or a trading operation, that response can be nearly as damaging as the attack.

What selective suspension achieves

The attack is suspended in memory. Legitimate transactions never stop. In the financial services deployment where nearly 10,000 malicious processes were intercepted, legitimate SQL transactions continued uninterrupted throughout — operations were never taken down.

This is what makes prevention compatible with business continuity rather than a trade-off against it.

Revision #3
Created 2026-07-20 19:23:55 UTC by Dennis Underwood
Updated 2026-07-21 19:32:11 UTC by Dennis Underwood